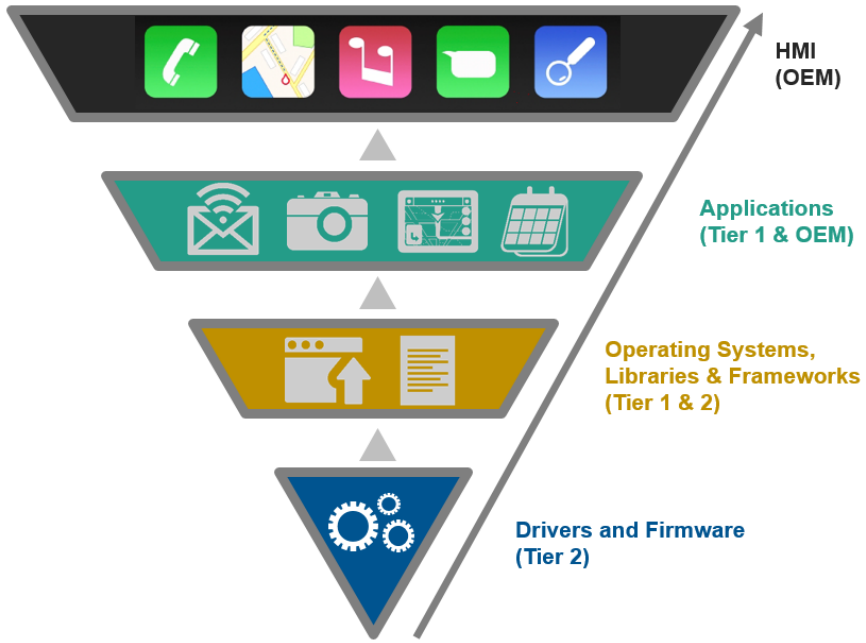
SYNOPSYS®
Silicon to Software™

Cybersecurity Assurance Testing Task Force

Mike Ahmadi
Global Director, Critical Systems Security
Synopsys Software Integrity Group

An Automobile Is The Result Of A Large Supply Chain

Software Supply Chain

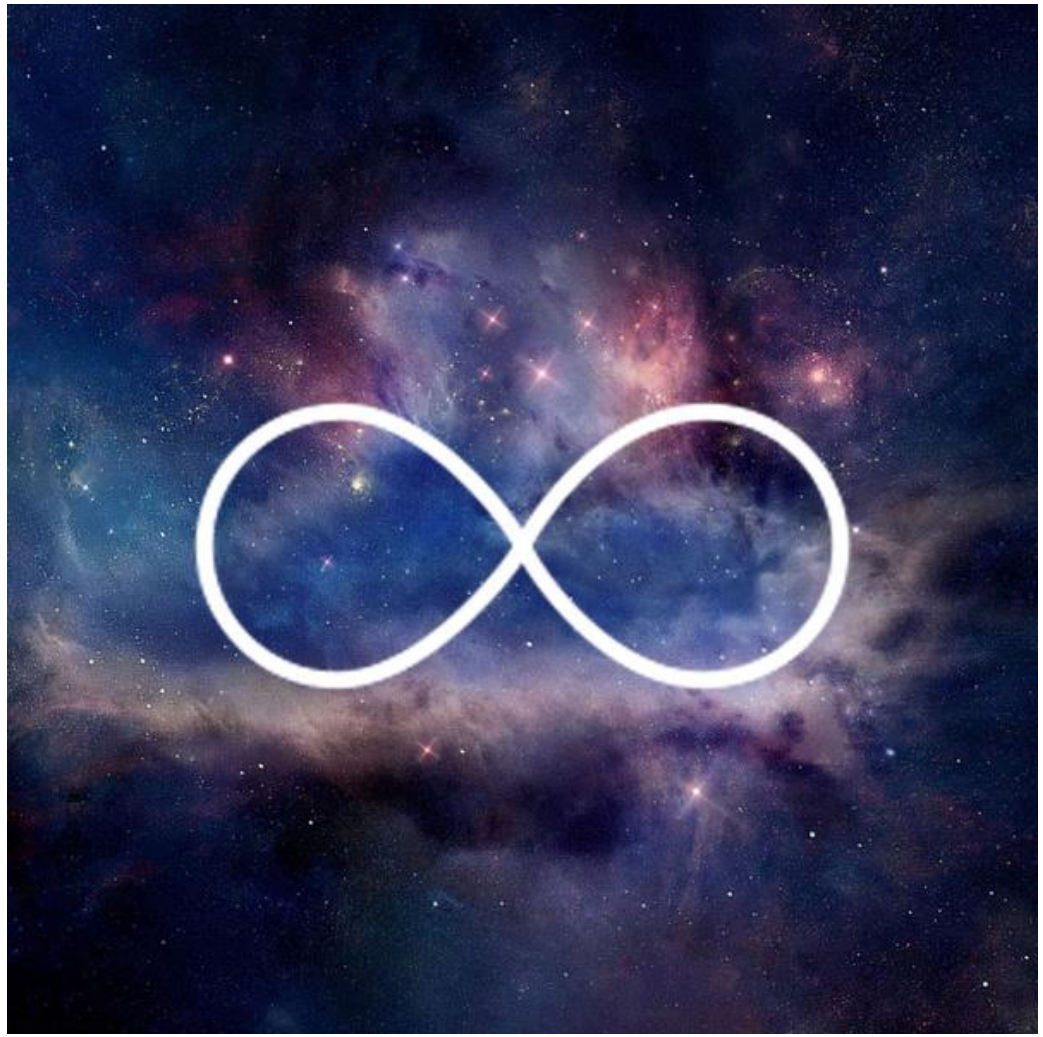


Security Attack Scenario

- Malware attacks via communication channels
- Attacks from downloaded apps and mobile apps
- Sniffing user data through keypads
- Malicious firmware update
- Web browser attacks
- Attacks on vehicle buses

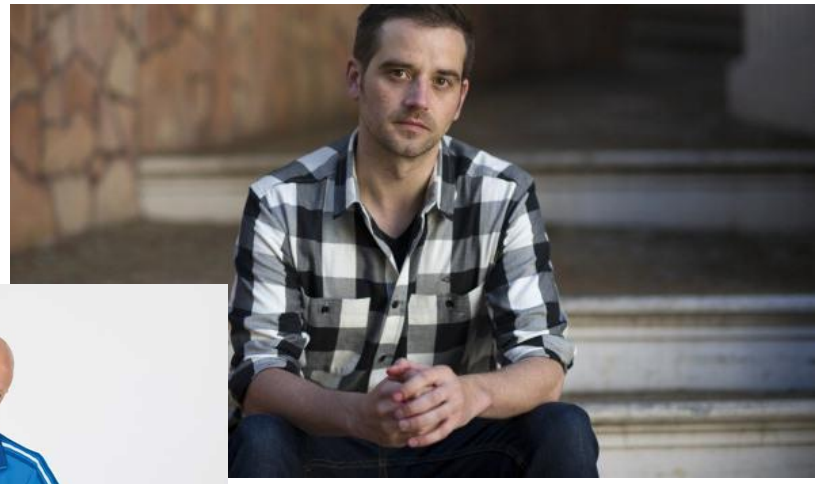
Why We Need Standardized Testing

- Cybersecurity is an infinite space problem.
- It is only through the application of proper practices AND rigorous validation and verification that we can derive some level of cyber-assurance.
- The testing methods have to be rigorous, consistent, and equitable.



We Can Be Certain Testing Will Happen

- The “dark wizards” of the world of security research love to test your security.
- ”I would do this even if I had to do if for free.” – Billy Rios
- Security researchers are a good thing…
- …yet it is better to find bugs before they do…or before the malicious hacker does.



SYNOPSYS®

About Testing: Ultimately It Comes Down To Who Is More Committed and Passionate

Or

TOYOTA

GM

Ford

HONDA

HARMAN

NISSAN

DELPHI
Innovation for the Real World

FCA
FIAT CHRYSLER AUTOMOBILES

BOSCH

It Began With Procurement Language: Setting Expectations In The Supply Chain

- Give the supplier a list of cyber security requirements to follow
- Verify that what is delivered meets the requirements
- This needs to be achievable, consistent, and based on standards
- Must be a continual work in progress that is flexible enough to change over time.

Supply Chain Cyber Assurance – Supplier Requirements

Introduction
This document serves as a minimal set of requirements for any supplier providing network-connectable software, systems, or devices as part of a contractual bid to Fiat Chrysler Automobiles (hereinafter referred to as FCA). A description of the required methods by which features and functions of network-connectable devices are expected to be evaluated at the product level and tested for known vulnerabilities and software security weaknesses while also establishing a minimum set of verification activities intended to reduce the likelihood of exploitable weaknesses that could be vectors of zero-day exploits that may affect the device are articulated throughout this document. While this document serves as a minimal set of requirements, FCA expects that suppliers will remain conscious of the dynamic nature of cybersecurity and provide incremental improvements as needed, which FCA shall consider for inclusion in future versions of this document. Suppliers shall be required to provide FCA with any and all requested artifacts as evidence that the supplier is in compliance with stated requirements.

Scope
These requirements applies to (but is not limited to) the following :
Application software
Embedded software
Firmware
Drivers
Middleware
Operating Systems
The requirements in this document are derived from various industry standards, guidelines, and other documents including, but not limited to:
IEC 62443
ISO 27001
NIST SP 800-53
NIST SP 800-82
DHS Cyber Security Procurement Language for Control Systems
ISA EDSA
FIPS 140-2
Common Criteria Smartcard IC Platform Protection Profile
Mayo Clinic Technology and Security Requirements Procurement Language
UL 2900
The requirements in this document apply to devices, software or software services that will be referred to as “product” throughout this document. The product can be connected to a network (public or private) and may be used as part of a system. These requirements are applicable to products that contain Do we really need to have this here

The Need For Performance-based Cybersecurity Testing Standards

- Best practices standards lack specifics on verification of security from a performance basis.
- Security researchers (aka Hackers) are doing the verification after products are fielded in a manner that the manufacturers and end users cannot control.
- Performance-based cybersecurity testing standards are well aligned with how the automotive industry builds products.
- Setting expectations is both fair and sensible.

Expect what you inspect !

SAE Cybersecurity Assurance Testing Requirements Task Force
Timeline To Launch

Mike Ahmadi is invited to lead SAE Task Force
Group formed under Vehicle Cybersecurity Systems Engineering Committee

March 15 2016

SAE incorporated an official task force to add cybersecurity testing requirements to SAE standards
First official meeting took place

Feb 2016

March 2016

RSA: "Featherstone Working Group"
Face-to-face meeting (likely to merge with the SAE working group)

RSA Conference 2016
Moscone Center, San Francisco
February 29 – March 4, 2016

Dec 4 2015

"Featherstone Working Group" first meeting:
Creation of a grassroots task force with multiple automotive industry stakeholders to address the need for cybersecurity testing standards

Dec 3 2015

SAE International hosted a global discussion on vehicle cybersecurity

"SAE J3061™:
Cybersecurity Guidebook for Cyber-Physical Vehicle Systems."

July/Aug 2015

Black Hat USA 2015:
The full story of how that Jeep was hacked

TEVEES18A1 SAE Cybersecurity Assurance Testing Task Force Charter

The members of this working group propose to establish a task force for the purpose of investigating Cybersecurity Assurance Testing. The charter of this task force is defined as follows:

- **Develop** appropriate SAE **documentation** for cybersecurity assurance testing and evaluation
- The task force shall become more familiar with what **types of testing** and evaluations **are effective** in measuring claims of cybersecurity development practices and mechanisms
- The task force shall work towards creating a consistent framework where **all systems and components** throughout the extended supply chain are **evaluated with a common set of criteria**
- The goal is to produce a common means of evaluation criteria wherein Stakeholders can **sign off on the hardware and software configuration** received with confidence that the **expected level of cybersecurity** evaluation criteria has been met.
- The subcommittee shall **leverage existing work** that has been previously accomplished by security **experts and testing organizations**

http://www.sae.org/servlets/works/committeeHome.do?comtID=TEVEES18A1

Our Approach – Existing Standards and Recommendations

CWE

IEC

CWE and SANS Institute TOP 25 MOST DANGEROUS SOFTWARE ERRORS

ISO

CVE cve.mitre.org

Microsoft SDL

NIST National Institute of Standards and Technology

IEEE

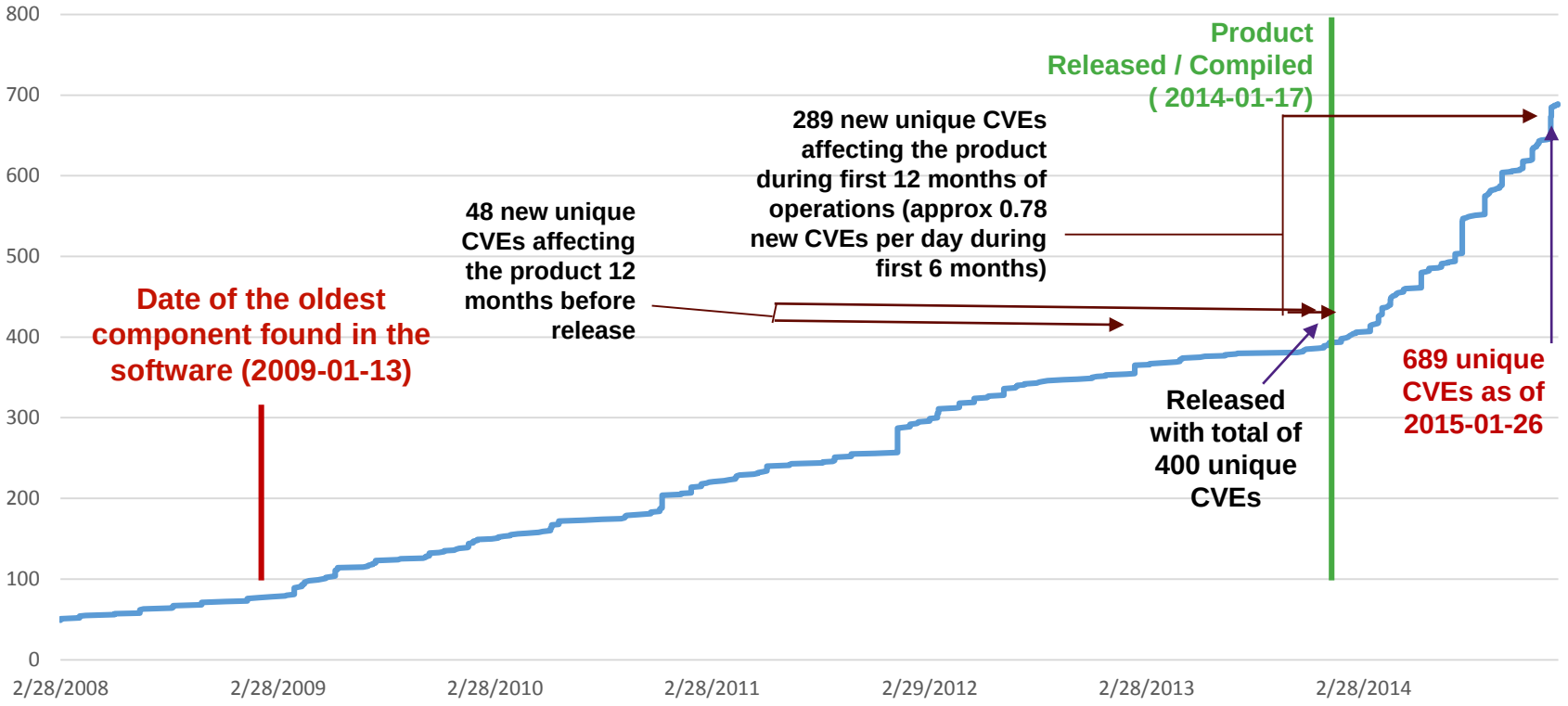
APEC

SAE INTERNATIONAL

OWASP Mobile Security Project

OWASP Open Web Application Security Project

Code decay over time – router



600% Increase In Unique Vulnerabilities Discovered In One Year

Vehicle Attack Surface Enumeration

Features

- Flexible Framework
- Utilizes Standards Definitions
- Can be automated
- Can be event driven or level driven

Security Testing Technique	Security Testing Tool
Review	
Network Sniffing	Dsniff, Ettercap, Kismet, Mailsnarf, Msgsnarf, Ntop, Phoss, SinFP, SMB Sniffer, and Wireshark
File Integrity Checking	Autopsy, Foremost, RootkitHunter, and Sleuthkit
Target Identification and Analysis	
Application Security Testing	CIRT Fuzzer, Fuzzer 1.2, NetSed, Paros Proxy, and Peach
Network Discovery	Autonomous System Scanner, Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Nmap, P0f, Tctrace, and Umit
Network Port and Service Identification	Amap, AutoScan, Netdiscover, Nmap, P0f, Umit, and UnicornScan
Vulnerab	
Wireless	
Target V	
Passwo	
Remote	
Penetrat	

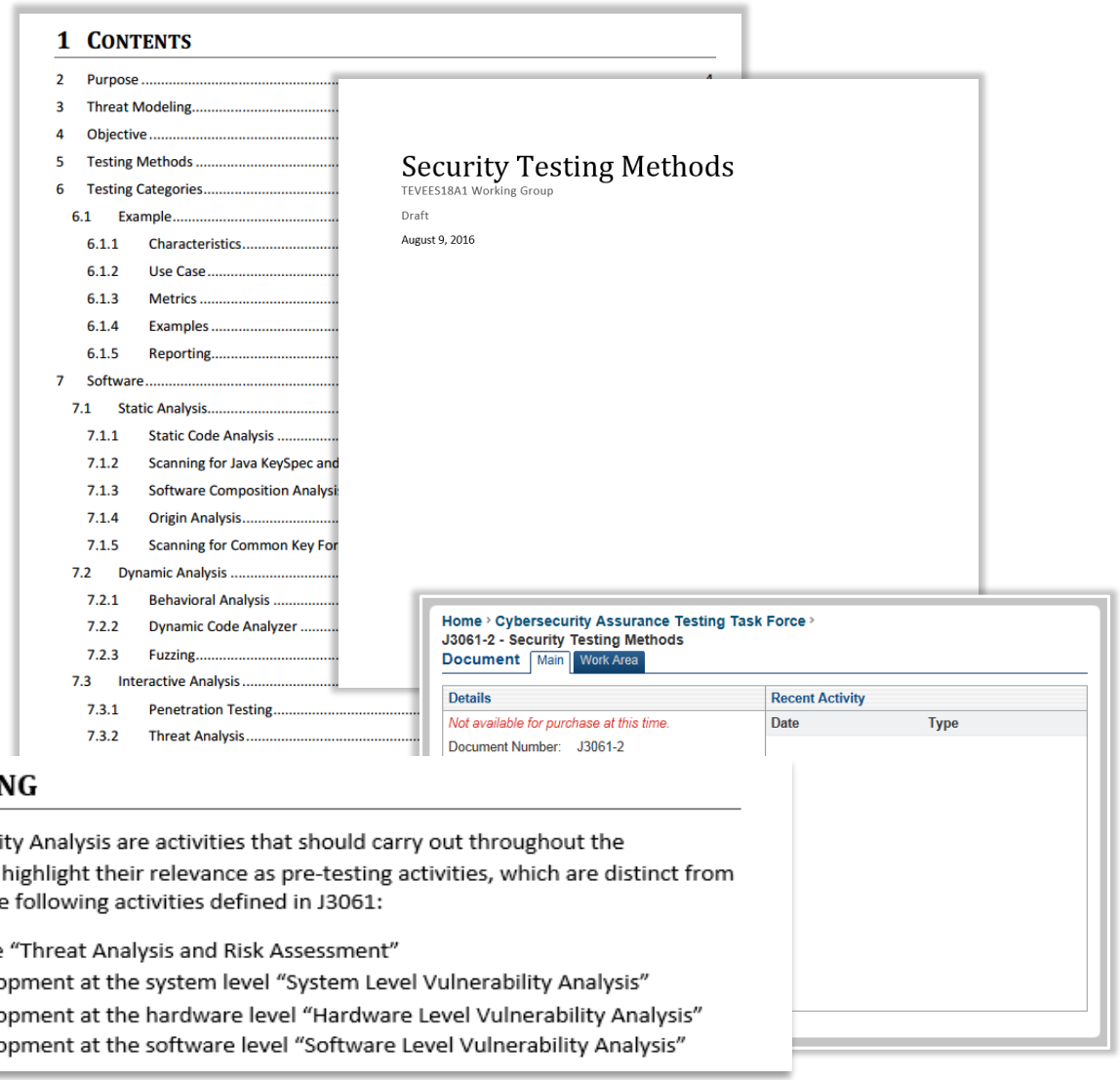
	C	D	E	F	G	H	I	J
1	New	New	New				NEW	NEW
2	Identifier	Zone	Path	Attack Narrative	CAPEC Categories	Associated CAPEC	CVE - Know Vulnerability	CWE - https://cwe.mitre.org/
3	1		rf>bluetooth.rfchip.infotainmnet	Conduit for malicious/malformed attack payload to trigger other flaws. Exfiltration of sensitive data or IP. Vector for malicious reprogramming or updates via physical interception/man-in-the-middle attacks. Software flaws in hardware drivers or hardware implementation leading to system-level control (e.g. 'Bad USB').	CATEGORY 345: Content Spoofing CATEGORY 255: Manipulate Data Structures CATEGORY 2: Inducing Lockout CATEGORY 513: Software	CAPEC-148: Content Spoofing CAPEC-123: Buffer Manipulation CAPEC-212: Functionality Misuse		
4	2		vehicle.wifi>wifi.rfchip.infotainmnet.canbus.ecu	Wi-Fi auto-probing functionality. Network impersonation attacks. Traffic man-in-the-middle. Server/service impersonation. Transmission of other attack payloads (i.e. malformed application-layer data, network layer service attacks). Tracking and monitoring.	CATEGORY 232: Exploitation of Authorization CATEGORY 118: Gather Information CATEGORY 286: Reconnaissance	CAPEC-28: Fuzzing CAPEC-94: Man in the Middle CAPEC-22: Exploiting Trust in Client CAPEC-312: Active OS Fingerprinting CAPEC-613: Wi-Fi SSID Tracking CAPEC-619: Signal Strength Tracking		
5	3			Obtain additional network entry point. Billing impact for service charges, etc. Malicious device may 'man in the middle' data from other devices (i.e. tablets and phones).	CATEGORY 281: Analyze Target CATEGORY 286: Reconnaissance	CAPEC-37: Retrieve Embedded Sensitive Data CAPEC-170: Web Application Fingerprinting CAPEC-205: Lifting credential(s)/key material embedded in client distributions (thick or thin) CAPEC-310: Scanning for Vulnerable Software CAPEC-563: Add Malicious File to Shared Webroot CAPEC-571: Block Logging to Central Repository		

SYNOPSYS®

J3061-2: Security Testing Methods

Features

- Active development
- OEM, Tier1-3, Security community participation
- Active Work In Progress documents

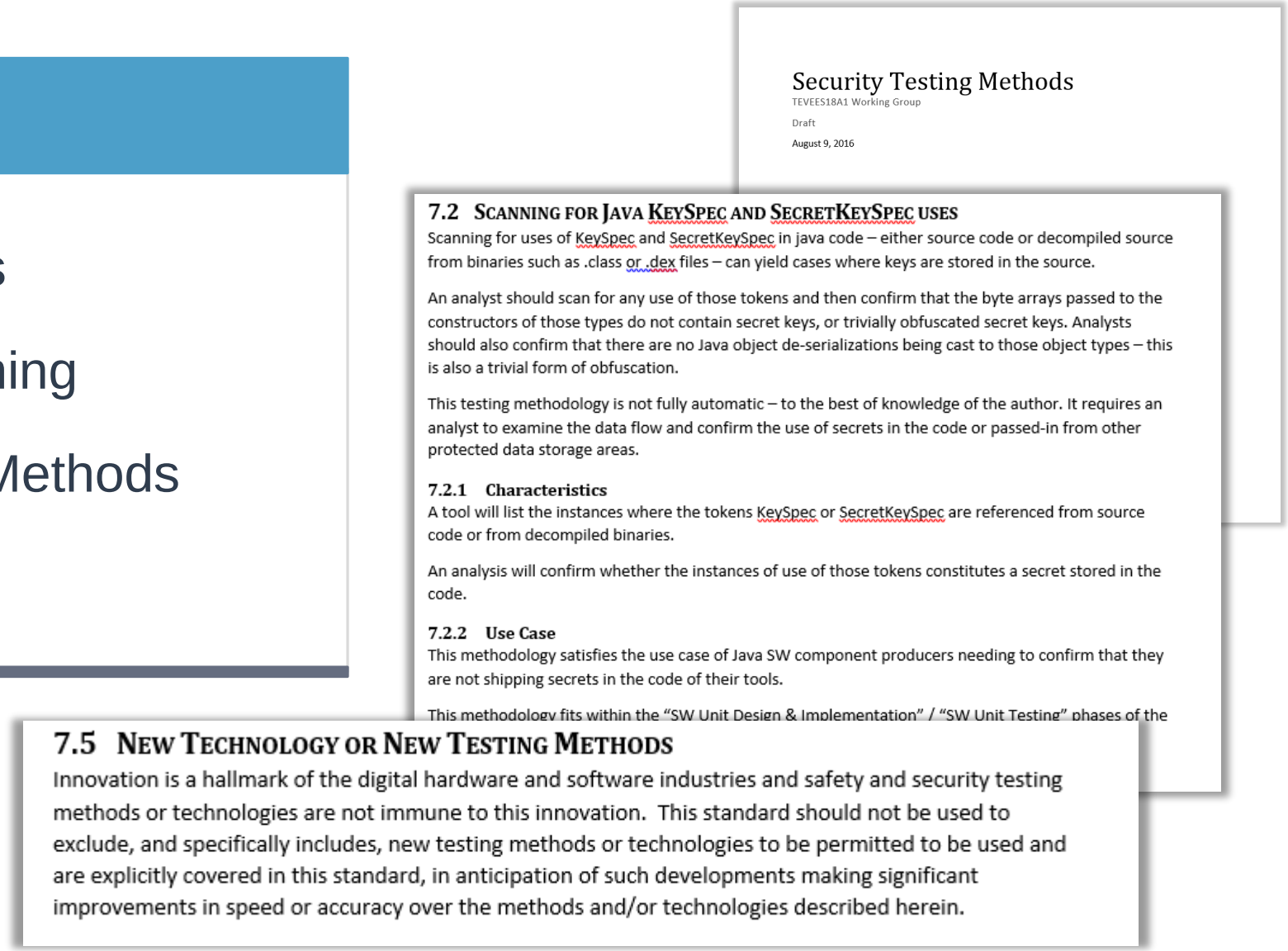


SYNOPSYS®

J3061-2: Security Testing Methods

Example

- Security Testing Methods
- 7.2 Java KeySpec Scanning
- Future Proofing Testing Methods



Security Testing Methods

TEVEES18A1 Working Group

Draft

August 9, 2016

7.2 Scanning for Java KeySpec and SecretKeySpec uses

Scanning for uses of KeySpec and SecretKeySpec in java code – either source code or decompiled source from binaries such as .class or .dex files – can yield cases where keys are stored in the source.

An analyst should scan for any use of those tokens and then confirm that the byte arrays passed to the constructors of those types do not contain secret keys, or trivially obfuscated secret keys. Analysts should also confirm that there are no Java object de-serializations being cast to those object types – this is also a trivial form of obfuscation.

This testing methodology is not fully automatic – to the best of knowledge of the author. It requires an analyst to examine the data flow and confirm the use of secrets in the code or passed-in from other protected data storage areas.

7.2.1 Characteristics

A tool will list the instances where the tokens KeySpec or SecretKeySpec are referenced from source code or from decompiled binaries.

An analysis will confirm whether the instances of use of those tokens constitutes a secret stored in the code.

7.2.2 Use Case

This methodology satisfies the use case of Java SW component producers needing to confirm that they are not shipping secrets in the code of their tools.

This methodology fits within the "SW Unit Design & Implementation" / "SW Unit Testing" phases of the

7.5 New Technology or New Testing Methods

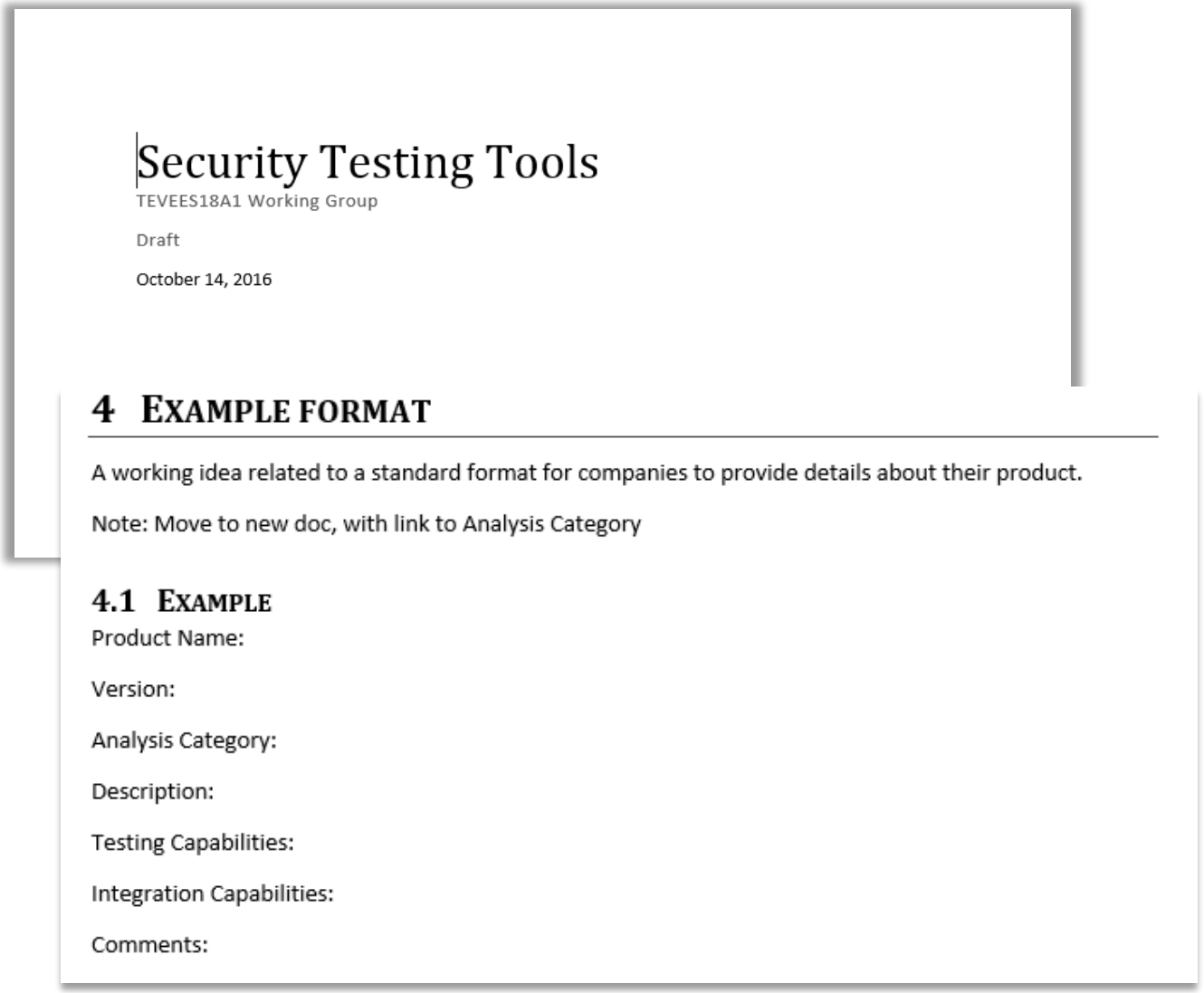
Innovation is a hallmark of the digital hardware and software industries and safety and security testing methods or technologies are not immune to this innovation. This standard should not be used to exclude, and specifically includes, new testing methods or technologies to be permitted to be used and are explicitly covered in this standard, in anticipation of such developments making significant improvements in speed or accuracy over the methods and/or technologies described herein.

SYNOPSYS®

J3061-3: Vendor Testing Tools

Features

- Specific Tools, Capabilities and Vendors
- Categorized capabilities
- Simple maintenance (continual work in progress
- Not part of the standard – To remain informative



Security Testing Tools

TEVEES18A1 Working Group

Draft

October 14, 2016

4 EXAMPLE FORMAT

A working idea related to a standard format for companies to provide details about their product.

Note: Move to new doc, with link to Analysis Category

4.1 EXAMPLE

Product Name:

Version:

Analysis Category:

Description:

Testing Capabilities:

Integration Capabilities:

Comments:

SYNOPSYS®

Joint Standard Development Between SAE/ISO

- SAE and ISO have agreed to partner to develop a joint standard based on the SAE cybersecurity task force work products
- The fist meeting was held in Munich from October 19 – October 21 2016
- Each participating country will submit 10 members to participate in the meetings.
- Next meeting in Silicon Valley on March 2-3, 2017

SYNOPSYS®
Silicon to Software™

Thank You